

# **SELF-GENERATION OF PUBLIC/PRIVATE KEY PAIRS USING A SECURE MICROPROCESSOR IN A DEVICE FOR TRANSFERRING ENCODED INFORMATION OVER A NETWORK**

5

## **ABSTRACT OF THE DISCLOSURE**

Devices in a telecommunications system are provided with means to self-generate public key pairs and certificates. This eliminates the need for such keys and certificates to be sent to the devices from an outside source so a single-trust approach can be maintained. A manufacturer's certificate is installed into a device at the time of manufacture.

10

The device only issues itself certificates based on a signed request from an external outside server. The device's self-issued certificates incorporate information obtained from the server in a profile. This allows control by the server over a device's self-issued certificates. In order to prevent tampering, and breaking, of the self-issued certificates, the certificate issuing process occurs within a secure microprocessor.

15